PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-069598
(43)Date of publication of application : 07.03.2003

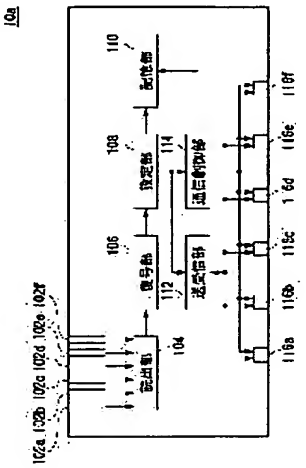
(51)Int.Cl. H04L 12/46

(21)Application number : 2001-253225
(22)Date of filing : 23.08.2001

(71)Applicant : ALLIED TERESHISU KK
(72)Inventor : SATO TAKAYUKI
HANEDA JUN

(54) RELAY APPARATUS, COMMUNICATION SETTING PROGRAM, AND COMMUNICATION SETTING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a relay apparatus realizing a computer network system which is very high in security against unauthorized access.
SOLUTION: The relay apparatus, which relays communication in a computer network, is provided with the first holding portion for holding a removable nonvolatile memory, a reading portion for reading, from the nonvolatile memory held in a first holding portion, a first apparatus identifying information of a first communication apparatus to which the communication in the computer network is permitted, and a setting portion for performing a communication setting of the computer network in order to permit the communication in the computer network of the first communication apparatus identified by the first apparatus identifying information.



LEGAL STATUS

[Date of request for examination] 29.10.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－69598
（Ｐ２００３－６９５９８Ａ）
(43)公開日　平成15年３月７日(2003.3.7)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
H04L 12/46	100	H04L 12/46	100	B 5K033

審査請求　未請求　請求項の数18　ＯＬ　（全10頁）

(21)出願番号　特願2001－253225（Ｐ2001－253225）

(22)出願日　平成13年８月23日(2001.8.23)

(71)出願人　396008347
アライドテレシス株式会社
東京都品川区西五反田７－22－17　ＴＯＣビル

(72)発明者　佐藤　貴之
東京都品川区西五反田７－22－17　ＴＯＣビル　アライドテレシス株式会社内

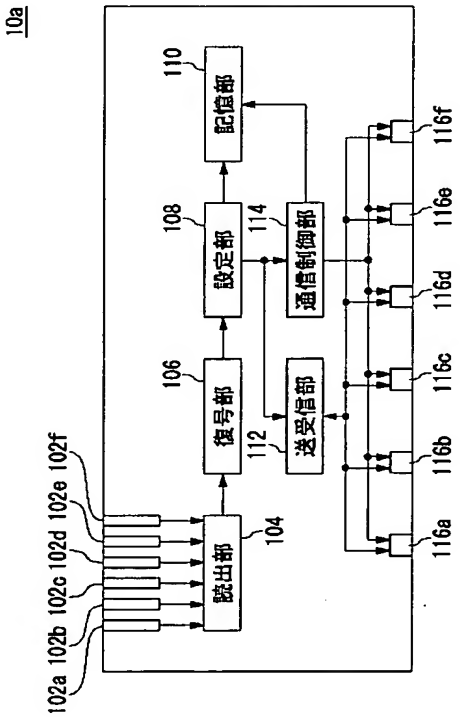
(72)発明者　羽田　純
東京都品川区西五反田７－22－17　ＴＯＣビル　アライドテレシス株式会社内

(74)代理人　100104156
弁理士　龍華　明裕

Ｆターム(参考)　5K033 AA08 BA04 CB08 CC01 DA05 DB10 DB18

(54)【発明の名称】中継機器、通信設定プログラム、及び通信設定方法

(57)【要約】
【課題】　不正進入に対するセキュリティが非常に高いコンピュータネットワークシステムを実現できる中継機器を提供する。
【解決手段】　コンピュータネットワークにおいて通信を中継する中継機器であって、着脱可能な不揮発性メモリを保持する第１保持部と、第１保持部に保持された不揮発性メモリから、コンピュータネットワークにおける通信が許可される第１通信機器の第１機器識別情報を読み出す読出部と、第１機器識別情報で識別される第１通信機器のコンピュータネットワークにおける通信を許可すべくコンピュータネットワークの通信設定を行う設定部とを備える。



1

【特許請求の範囲】

【請求項１】　コンピュータネットワークにおいて通信を中継する中継機器であって、

着脱可能な不揮発性メモリを保持する第１保持部と、

前記第１保持部に保持された前記不揮発性メモリから、前記コンピュータネットワークにおける通信が許可される第１通信機器の第１機器識別情報を読み出す読出部と、

前記第１機器識別情報で識別される前記第１通信機器の前記コンピュータネットワークにおける通信を許可すべく前記コンピュータネットワークの通信設定を行う設定部とを備えることを特徴とする中継機器。

【請求項２】　前記不揮発性メモリは、暗号化された前記第１機器識別情報を格納し、

前記読出部に読み出された前記第１機器識別情報を復号する復号部をさらに備えることを特徴とする請求項１に記載の中継機器。

【請求項３】　前記設定部は、前記第１機器識別情報で識別される前記第１通信機器の当該中継機器における通信を許可すべく当該中継機器を設定することを特徴とする請求項１に記載の中継機器。

【請求項４】　前記設定部は、前記第１機器識別情報で識別される前記第１通信機器による通信の、当該中継機器における帯域幅をさらに設定することを特徴とする請求項３に記載の中継機器。

【請求項５】　前記第１機器識別情報で識別される前記第１通信機器の当該中継機器に接続された他の中継機器における通信を許可させるように設定させるべく、前記第１機器識別情報を前記他の中継機器に送信する送信部をさらに備えることを特徴とする請求項３に記載の中継機器。

【請求項６】　前記他の中継機器は、前記コンピュータネットワークと、前記コンピュータネットワークの他のコンピュータネットワークとを接続しており、

前記送信部は、前記第１機器識別情報で識別される前記第１通信機器の前記他のコンピュータネットワークにおける通信を許可させるように設定させるべく、前記第１機器識別情報を前記他の中継機器に送信することを特徴とする請求項５に記載の中継機器。

【請求項７】　前記第１機器識別情報で識別される前記第１通信機器の前記コンピュータネットワークにおける通信を許可するように設定させるべく、前記コンピュータネットワークを管理する管理装置に、前記第１機器識別情報を送信する送信部をさらに備えることを特徴とする請求項３に記載の中継機器。

【請求項８】　着脱可能な不揮発性メモリを保持する第２保持部をさらに有し、

前記読出部は、前記第２保持部に保持された前記不揮発性メモリから、前記コンピュータネットワークにおける通信が許可される第２通信機器の第２機器識別情報を読み出し、

2

前記設定部は、前記第２機器識別情報で識別される前記第２通信機器の前記コンピュータネットワークにおける通信を許可すべく前記コンピュータネットワークの前記通信設定を行うことを特徴とする請求項１に記載の中継機器。

【請求項９】　前記設定部は、前記第１機器識別情報で識別される前記第１通信機器の当該中継機器における前記通信を許可すべく当該中継機器を設定し、前記第２機器識別情報で識別される前記第２通信機器の当該中継機器における前記通信を許可すべく当該中継機器を設定することを特徴とする請求項８に記載の中継機器。

【請求項１０】　前記第１通信機器が接続される第１接続ポートと、

前記第２通信機器が接続される第２接続ポートとをさらに備え、

前記設定部は、前記第１通信機器の前記第１接続ポートにおける通信と、前記第２通信機器の前記第２接続ポートにおける通信とを許可すべく、当該中継機器を設定することを特徴とする請求項９に記載の中継機器。

【請求項１１】　前記設定部は、前記第１接続ポート及び前記第２接続ポートを介する通信の帯域幅をさらに設定することを特徴とする請求項１０に記載の中継機器。

【請求項１２】　当該中継機器における通信を許可する少なくとも１つの通信機器の機器識別情報を格納する記憶部と、

前記記憶部に格納された前記機器識別情報に基づいて、当該中継機器における通信を許可する通信機器を制限する通信制御部とをさらに備えることを特徴とする請求項１に記載の中継機器。

【請求項１３】　前記設定部は、前記読出部により読み出された前記第１機器識別情報で識別される前記第１通信機器の当該中継機器における通信を許可すべく、前記読出部により読み出された前記第１機器識別情報を前記記憶部に格納することを特徴とする請求項１２に記載の中継機器。

【請求項１４】　当該中継機器は、複数の通信機器がそれぞれ接続される複数の接続ポートを有し、

前記記憶部は、前記複数の接続ポートのそれぞれに対応づけて、前記複数の接続ポートのそれぞれにおける通信を許可する少なくとも１つの通信機器の機器識別情報を格納することを特徴とする請求項１２に記載の中継機器。

【請求項１５】　コンピュータネットワークの通信設定を行う中継機器用の通信設定プログラムであって、前記中継機器に、

着脱可能な不揮発性メモリから、前記コンピュータネットワークにおける通信が許可される通信機器の機器識別情報を読み出させる読出モジュールと、

前記機器識別情報で識別される前記通信機器の前記コン

ピュータネットワークにおける通信を許可すべく前記コンピュータネットワークの通信設定を行わせる設定モジュールとを備えることを特徴とする通信設定プログラム。

【請求項１６】　前記設定モジュールは、前記機器識別情報で識別される前記通信機器の当該中継機器における通信を許可させるべく当該中継機器を設定させることを特徴とする請求項１５に記載の通信設定プログラム。

【請求項１７】　前記機器識別情報で識別される前記通信機器の当該中継機器に接続された他の中継機器における通信を許可させるように設定させるべく、前記機器識別情報を前記他の中継機器に送信させる送信モジュールをさらに備えることを特徴とする請求項１６に記載の通信設定プログラム。

【請求項１８】　コンピュータネットワークにおいて通信を中継する中継機器による前記コンピュータネットワークの通信設定方法であって、
着脱可能な不揮発性メモリを保持する保持段階と、
保持された前記不揮発性メモリから、前記コンピュータネットワークにおける通信が許可される通信機器の機器識別情報を読み出す読出段階と、
前記機器識別情報で識別される前記通信機器の前記コンピュータネットワークにおける通信を許可すべく前記コンピュータネットワークの通信設定を行う設定段階とを備えることを特徴とする通信設定方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、中継機器、通信設定プログラム、及び通信設定方法に関する。特に本発明は、コンピュータネットワークの通信設定を行う中継機器に関する。

【０００２】

【従来の技術】従来、コンピュータネットワークを統括的に管理する管理サーバによって、任意のコンピュータによるコンピュータネットワークへの不正進入に対するセキュリティが実現されている。例えば、管理サーバによるユーザ認証、ＶＬＡＮの設定等によってコンピュータネットワークへの進入の制限を行っている。

【０００３】

【発明が解決しようとする課題】しかしながら、従来のコンピュータネットワークシステムでは、管理サーバによってコンピュータネットワークへの進入を制限しているため、ユーザが使用する任意のコンピュータは、コンピュータネットワークを介して管理サーバに接続する。そのため、実質的に任意のコンピュータによるコンピュータネットワークへの進入を制限する手段はなく、任意のコンピュータが容易にコンピュータネットワークにおいて通信を行うことができるという問題がある。

【０００４】そこで本発明は、上記の課題を解決することのできる中継機器、通信設定プログラム、及び通信設定方法を提供することを目的とする。この目的は特許請求の範囲における独立項に記載の特徴の組み合わせにより達成される。また従属項は本発明の更なる有利な具体例を規定する。

【０００５】

【課題を解決するための手段】即ち、本発明の第１の形態によると、コンピュータネットワークにおいて通信を中継する中継機器であって、着脱可能な不揮発性メモリを保持する第１保持部と、第１保持部に保持された不揮発性メモリから、コンピュータネットワークにおける通信が許可される第１通信機器の第１機器識別情報を読み出す読出部と、第１機器識別情報で識別される第１通信機器のコンピュータネットワークにおける通信を許可すべくコンピュータネットワークの通信設定を行う設定部とを備える。

【０００６】不揮発性メモリは、暗号化された第１機器識別情報を格納し、読出部に読み出された第１機器識別情報を復号する復号部をさらに備えてもよい。設定部は、第１機器識別情報で識別される第１通信機器の当該中継機器における通信を許可すべく当該中継機器を設定してもよい。設定部は、第１機器識別情報で識別される第１通信機器による通信の、当該中継機器における帯域幅をさらに設定してもよい。

【０００７】第１機器識別情報で識別される第１通信機器の当該中継機器に接続された他の中継機器における通信を許可させるように設定させるべく、第１機器識別情報を他の中継機器に送信する送信部をさらに備えてもよい。

【０００８】他の中継機器は、コンピュータネットワークと、コンピュータネットワークの他のコンピュータネットワークとを接続しており、送信部は、第１機器識別情報で識別される第１通信機器の他のコンピュータネットワークにおける通信を許可させるように設定させるべく、第１機器識別情報を他の中継機器に送信してもよい。

【０００９】第１機器識別情報で識別される第１通信機器のコンピュータネットワークにおける通信を許可するように設定させるべく、コンピュータネットワークを管理する管理装置に、第１機器識別情報を送信する送信部をさらに備えてもよい。

【００１０】着脱可能な不揮発性メモリを保持する第２保持部をさらに有し、読出部は、第２保持部に保持された不揮発性メモリから、コンピュータネットワークにおける通信が許可される第２通信機器の第２機器識別情報を読み出し、設定部は、第２機器識別情報で識別される第２通信機器のコンピュータネットワークにおける通信を許可すべくコンピュータネットワークの通信設定を行ってもよい。

【００１１】設定部は、第１機器識別情報で識別される第１通信機器の当該中継機器における通信を許可すべく

当該中継機器を設定し、第２機器識別情報で識別される第２通信機器の当該中継機器における通信を許可すべく当該中継機器を設定してもよい。

【００１２】第１通信機器が接続される第１接続ポートと、第２通信機器が接続される第２接続ポートとをさらに備え、設定部は、第１通信機器の第１接続ポートにおける通信と、第２通信機器の第２接続ポートにおける通信とを許可すべく、当該中継機器を設定してもよい。設定部は、第１接続ポート及び第２接続ポートを介する通信の帯域幅をさらに設定してもよい。

【００１３】当該中継機器における通信を許可する少なくとも１つの通信機器の機器識別情報を格納する記憶部と、記憶部に格納された機器識別情報に基づいて、当該中継機器における通信を許可する通信機器を制限する通信制御部とをさらに備えてもよい。

【００１４】設定部は、読出部により読み出された第１機器識別情報で識別される第１通信機器の当該中継機器における通信を許可すべく、読出部により読み出された第１機器識別情報を記憶部に格納してもよい。

【００１５】当該中継機器は、複数の通信機器がそれぞれ接続される複数の接続ポートを有し、記憶部は、複数の接続ポートのそれぞれに対応づけて、複数の接続ポートのそれぞれにおける通信を許可する少なくとも１つの通信機器の機器識別情報を格納してもよい。

【００１６】本発明の第２の形態によると、コンピュータネットワークの通信設定を行う中継機器用の通信設定プログラムであって、中継機器に、着脱可能な不揮発性メモリから、コンピュータネットワークにおける通信が許可される通信機器の機器識別情報を読み出させる読出モジュールと、機器識別情報で識別される通信機器のコンピュータネットワークにおける通信を許可すべくコンピュータネットワークの通信設定を行わせる設定モジュールとを備える。

【００１７】設定モジュールは、機器識別情報で識別される通信機器の当該中継機器における通信を許可させるべく当該中継機器を設定させてもよい。

【００１８】機器識別情報で識別される通信機器の当該中継機器に接続された他の中継機器における通信を許可させるように設定させるべく、機器識別情報を他の中継機器に送信させる送信モジュールをさらに備えてもよい。

【００１９】本発明の第３の形態によると、コンピュータネットワークにおいて通信を中継する中継機器によるコンピュータネットワークの通信設定方法であって、着脱可能な不揮発性メモリを保持する保持段階と、保持された不揮発性メモリから、コンピュータネットワークにおける通信が許可される通信機器の機器識別情報を読み出す読出段階と、機器識別情報で識別される通信機器のコンピュータネットワークにおける通信を許可すべくコンピュータネットワークの通信設定を行う設定段階とを備える。

【００２０】なお上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではなく、これらの特徴群のサブコンビネーションも又発明となりうる。

【００２１】

【発明の実施の形態】以下、発明の実施形態を通じて本発明を説明するが、実施形態はクレームにかかる発明を限定するものではなく、また実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

【００２２】図１は、本発明の一実施形態に係るコンピュータネットワーク１００の構成を示す。本実施形態のコンピュータネットワーク１００は、コンピュータネットワーク１００における通信を中継するスイッチングハブ等の中継機器１０ａ及び１０ｂと、コンピュータネットワーク１００における通信を管理する管理装置２０と、コンピュータネットワーク１００において通信を行う通信機器３０ａ、３０ｂ、３０ｃ、及び３０ｄとを備える。

【００２３】中継機器１０ａ及び１０ｂは、ＩＣカード、ミニチュアカード、フロッピー（登録商標）ディスク等の不揮発性メモリからコンピュータネットワーク１００の設定情報を読み出し、コンピュータネットワーク１００の通信設定を行う。例えば、中継機器１０ａは、不揮発性メモリを保持する保持部の一例であるＩＣカードスロットを有し、通信機器３０ａを使用するユーザによって挿入されたＩＣカードから、通信機器３０ａの機器識別情報としてＭＡＣアドレスを読み出す。そして、中継機器１０ａは、ＩＣカードから読み出したＭＡＣアドレスで識別される通信機器３０ａの中継機器１０ａにおける通信を許可すべく、中継機器１０ａを設定する。

【００２４】つまり、通信機器３０ａを使用するユーザは、通信機器３０ａを用いてコンピュータネットワーク１００に接続するための鍵として、通信機器３０ａを識別するためのＭＡＣアドレスが格納されたＩＣカードを中継機器１０ａに挿入する。そして、ユーザは、ＩＣカードを中継機器１０ａに挿入した状態で通信機器３０ａを使用することにより、コンピュータネットワーク１００に進入することができる。また、ＩＣカードを中継機器１０ａから取り外した場合、ユーザは、通信機器３０ａによるコンピュータネットワーク１００の利用を制限される。例えば、ユーザは、通信機器３０ａによるコンピュータネットワーク１００への進入を禁止されてもよいし、通信機器３０ｂ、３０ｃ、又は３０ｃに格納されたデータの読み取り等の一定の動作だけが許容されてもよい。

【００２５】また、中継機器１０ａは、ＩＣカードから読み出したＭＡＣアドレスで識別される通信機器３０ａの中継機器１０ｂにおける通信を許可させるべく、ＩＣカードから読み出したＭＡＣアドレスを中継機器１０ｂ

に送信する。そして、中継機器１０ｂは、中継機器１０ａから受信したＭＡＣアドレスで識別される通信機器３０ａの中継機器１０ｂにおける通信を許可すべく、中継機器１０ｂを設定する。つまり、通信機器３０ａを使用するユーザは、通信機器３０ａを識別するためのＭＡＣアドレスが格納されたＩＣカードを中継機器１０ａに挿入することにより、通信機器３０ａを用いて、中継機器１０ｂに接続された通信機器３０ｃ及び３０ｄと通信することができる。

【００２６】また他の例では、中継機器１０ａは、ＩＣカードから読み出したＭＡＣアドレスで識別される通信機器３０ａのコンピュータネットワーク１００における通信を許可させるべく、ＩＣカードから読み出したＭＡＣアドレスを管理装置２０に送信する。そして、管理装置２０は、中継機器１０ａから受信したＭＡＣアドレスで識別される通信機器３０ａのコンピュータネットワーク１００における通信を許可させるべく、中継機器１０ａ及び１０ｂを設定する。そして、通信機器３０ａを使用するユーザは、通信機器３０ａを識別するためのＭＡＣアドレスが格納されたＩＣカードを中継機器１０ａに挿入することにより、通信機器３０ａを用いて、コンピュータネットワーク１００において通信することができる。

【００２７】本実施形態に係る中継機器１０ａ及び１０ｂによれば、所定のユーザが使用する所定の通信機器がコンピュータネットワーク１００に進入するための鍵である所定のＩＣカードを、所定のユーザが所持することによって、所定のＩＣカードを所持する所定のユーザのみに所定の通信機器によるコンピュータネットワーク１００への進入を許可することができる。したがって、所定の通信機器と所定のＩＣカードとの両方を所持する所定のユーザのみにコンピュータネットワーク１００への進入を許可することができるため、コンピュータネットワーク１００への不正進入を防ぐことができる。

【００２８】また、本実施形態に係るコンピュータネットワーク１００によれば、中継機器１０ａ及び１０ｂにおいて通信機器３０ａ、３０ｂ、３０ｃ、及び３０ｄによるコンピュータネットワーク１００への進入を制限するため、中継機器１０ａ及び１０ｂにおいて通信が許可されない通信機器は、管理装置２０への接続を許可させないこともできる。そのため、本実施形態係るコンピュータネットワーク１００によれば、不正進入に対するセキュリティが非常に高いコンピュータネットワークシステムを実現することができる。

【００２９】図２は、本実施形態に係る中継機器１０ａの構成を示す。中継機器１０ａと中継機器１０ｂとは、同一の構成を有しており、以下において、代表して中継機器１０ａの構成及び動作について説明する。

【００３０】中継機器１０ａは、着脱可能な不揮発性メモリを保持する保持部１０２ａ、１０２ｂ、１０２ｃ、１０２ｄ、１０２ｅ、及び１０２ｆと、不揮発性メモリから通信機器の機器識別情報を読み出す読出部１０４と、暗号化された機器識別情報を復号する復号部１０６と、読み出された機器識別情報で識別される通信機器のコンピュータネットワーク１００における通信を許可すべくコンピュータネットワーク１００の通信設定を行う設定部１０８と、中継機器１０ａにおける通信が許可された少なくとも１つの通信機器の機器識別情報を格納する記憶部１１０と、機器識別情報を送受信する送受信部１１２と、中継機器１０ａにおける通信を許可する通信機器を制限する通信制御部１１４と、通信機器が接続される接続ポート１１６ａ、１１６ｂ、１１６ｃ、１１６ｄ、１１６ｅ、及び１１６ｆとを備える。

【００３１】保持部１０２ａ、１０２ｂ、１０２ｃ、１０２ｄ、１０２ｅ、及び１０２ｆは、通信機器の機器識別情報が格納された不揮発性メモリを保持する。そして、読出部１０４は、保持部１０２ａ、１０２ｂ、１０２ｃ、１０２ｄ、１０２ｅ、又は１０２ｆに保持された不揮発性メモリから、コンピュータネットワーク１００における通信が許可される通信機器の機器識別情報を読み出す。復号部１０６は、不揮発性メモリから読み出された機器識別情報が暗号化されている場合、暗号化された機器識別情報を復号する。そして、復号部１０６は、復号した機器識別情報を設定部１０８に供給する。

【００３２】次に、設定部１０８は、不揮発性メモリから読み出された機器識別情報で識別される通信機器のコンピュータネットワーク１００における通信を許可すべくコンピュータネットワーク１００の通信設定を行う。まず、設定部１０８は、不揮発性メモリから読み出された機器識別情報で識別される通信機器の中継機器１０ａにおける通信を許可すべく、中継機器１０ａを設定する。具体的には、設定部１０８は、不揮発性メモリから読み出された機器識別情報を記憶部１１０に格納することにより、不揮発性メモリから読み出された機器識別情報で識別される通信機器の中継機器１０ａにおける通信を可能にする。

【００３３】次に、通信制御部１１４は、記憶部１１０に格納された機器識別情報に基づいて、中継機器１０ａにおける通信を許可する通信機器を制限する。つまり、通信制御部１１４は、不揮発性メモリから読み出され、記憶部１１０に格納された機器識別情報で識別される通信機器の中継機器１０ａにおける通信を許可する。例えば、通信制御部１１４は、送受信部１１２によって受信されたデータのヘッダ情報を参照し、ヘッダ情報に含まれる送信元の通信機器の機器識別情報が記憶部１１０に格納されている場合、送受信部１１２に対して当該データの送信を許可する。

【００３４】また、送受信部１１２は、中継機器１０ａにおける通信を許可する通信機器の機器識別情報を中継機器１０ｂから受信する。そして、設定部１０８は、送

受信部１１２が受信した機器識別情報を記憶部１１０に格納することにより、送受信部１１２が受信した機器識別情報で識別される通信機器の中継機器１０ａにおける通信を可能にする。

【００３５】また、送受信部１１２は、不揮発性メモリから読み出された機器識別情報で識別される通信機器の、中継機器１０ａに接続された中継機器１０ｂにおける通信を許可させるべく、不揮発性メモリから読み出された機器識別情報を中継機器１０ｂに送信してもよい。また、送受信部１１２は、不揮発性メモリから読み出された機器識別情報で識別される通信機器の、コンピュータネットワーク１００における通信を許可するように設定させるべく、コンピュータネットワーク１００を管理する管理装置２０に、不揮発性メモリから読み出された機器識別情報を送信してもよい。

【００３６】また、設定部１０８は、不揮発性メモリから読み出された機器識別情報で識別される通信機器による通信の、中継機器１０ａにおける帯域幅を設定してもよい。例えば、設定部１０８は、複数の接続ポートのそれぞれに対して、優先順位を設定してもよい。また、設定部１０８は、複数の接続ポートのそれぞれに対して、帯域幅の上限を設定してもよい。

【００３７】また、保持部１０２ａ、１０２ｂ、１０２ｃ、１０２ｄ、１０２ｅ、及び１０２ｆのそれぞれと、接続ポート１１６ａ、１１６ｂ、１１６ｃ、１１６ｄ、１１６ｅ、及び１１６ｆのそれぞれとは、対応づけられてもよい。つまり、通信制御部１１４は、保持部１０２ａに保持された不揮発性メモリから読み出された機器識別情報に基づいて、接続ポート１１６ａに接続された通信機器の中継機器１０ａにおける通信を制限し、保持部１０２ｂに保持された不揮発性メモリから読み出された機器識別情報に基づいて、接続ポート１１６ｂに接続された通信機器の中継機器１０ａにおける通信を制限してもよい。

【００３８】例えば、読出部１０４は、保持部１０２ａに保持された不揮発性メモリから、コンピュータネットワーク１００における通信が許可される通信機器３０ａの機器識別情報を読み出す。また、読出部１０４は、保持部１０２ｂに保持された不揮発性メモリから、コンピュータネットワーク１００における通信が許可される通信機器３０ｂの機器識別情報を読み出す。

【００３９】次に、設定部１０８は、保持部１０２ａに保持された不揮発性メモリから読み出された機器識別情報で識別される通信機器３０ａによる接続ポート１１６ａにおける通信を許可すべく、記憶部１１０に機器識別情報を格納する。また、設定部１０８は、保持部１０２ｂに保持された不揮発性メモリから読み出された機器識別情報で識別される通信機器３０ｂによる接続ポート１１６ｂにおける通信を許可すべく、記憶部１１０に機器識別情報を格納する。そして、通信制御部１１４は、記憶部１１０に格納された機器識別情報に基づいて、通信を許可する通信機器を制限する。

【００４０】また、通信制御部１１４は、中継機器１０ｂの保持部に保持された不揮発性メモリから読み出された機器識別情報に基づいて、中継機器１０ｂに接続された通信機器３０ｃ及び３０ｄの中継機器１０ａにおける通信を制限してもよい。また、設定部１０８は、接続ポート１１６ａ、１１６ｂ、１１６ｃ、１１６ｄ、１１６ｅ、及び１１６ｆを介する通信の帯域幅を設定してもよい。

【００４１】本実施形態に係る中継機器１０ａによれば、不揮発性メモリから、暗号化された通信機器の機器識別情報を読み出して復号するため、不揮発性メモリに格納された機器識別情報の漏洩を防ぐことができる。また、本実施形態に係る中継機器１０ａによれば、中継機器１０ａに挿入された不揮発性メモリに格納された設定情報に基づいて、通信機器毎又は接続ポート毎の中継機器１０ａにおける帯域幅を設定できるため、コンピュータネットワーク１００における通信路を効率的に利用することができる。また、本実施形態に係るコンピュータネットワーク１００によれば、中継機器毎にそれぞれの中継機器における通信が許可された通信機器を制限するため、不正進入に対するセキュリティが非常に高いコンピュータネットワークシステムを実現することができる。

【００４２】図３は、記憶部１１０に格納される通信制御ファイルのデータフォーマットの一例を示す。通信制御ファイルは、接続ポート番号フィールド及び機器識別情報フィールドを有する。接続ポート番号フィールドは、通信機器が有する複数の接続ポートを識別するために割り当てられた接続ポート番号を格納する。機器識別情報フィールドは、通信機器を識別するための識別情報を格納する。例えば、機器識別情報フィールドは、ＭＡＣアドレスを格納する。

【００４３】なお、本実施形態において、接続ポート１１６ａの接続ポート番号は１、接続ポート１１６ｂの接続ポート番号は２、接続ポート１１６ｃの接続ポート番号は３、接続ポート１１６ｄの接続ポート番号は４、接続ポート１１６ｅの接続ポート番号は５、接続ポート１１６ｆの接続ポート番号は６とする。

【００４４】通信制御ファイルは、複数の接続ポートのそれぞれに対応づけて、複数の接続ポートのそれぞれにおける通信を許可する少なくとも１つの通信機器の機器識別情報を格納する。例えば、通信制御部１１４は、所定の接続ポートから受信したデータのヘッダ情報を参照し、ヘッダ情報に含まれる送信元の通信機器の機器識別情報が、前記所定の接続ポートに対応づけて格納されている場合、送受信部１１２に対して当該データの送信を許可する。

【００４５】また、通信機器を識別する機器識別情報を

格納する不揮発性メモリが、通信機器を使用するユーザによって、保持部１０２ａ、１０２ｂ、１０２ｃ、１０２ｄ、１０２ｅ、又は１０２ｆに挿入されることにより、不揮発性メモリに格納された機器識別情報が通信制御ファイルに格納される。また、ユーザによって、保持部１０２ａ、１０２ｂ、１０２ｃ、１０２ｄ、１０２ｅ、又は１０２ｆから不揮発性メモリが取り外されることによって、不揮発性メモリに格納された機器識別情報が通信制御ファイルから削除される。

【００４６】通信制御部１１４は、機器識別情報１Ａ２５１Ｆ３３２６２Ｄで識別される通信機器の、接続ポート番号が１である接続ポート１１６ａにおける通信を許可する。また、通信制御部１１４は、機器識別情報３Ｆ３６１０１５２Ａ１Ｂで識別される通信機器の、接続ポート番号が２である接続ポート１１６ｂにおける通信を許可する。また、通信制御部１１４は、機器識別情報２Ｂ１Ａ３９２Ａ１８１Ｃで識別される通信機器の、接続ポート番号が４である接続ポート１１６ｄにおける通信を許可する。

【００４７】また、通信制御部１１４は、機器識別情報１Ｃ２Ａ３６１Ｆ２５３Ｂで識別される通信機器、及び機器識別情報２Ｂ２Ｄ２Ａ１５３６１Ｆで識別される通信機器の、接続ポート番号が６である接続ポート１１６ｆにおける通信が許可される。これは、接続ポート１１６ｆに接続された中継機器１０ｂの接続ポートに機器識別情報１Ｃ２Ａ３６１Ｆ２５３Ｂで識別される通信機器、及び機器識別情報２Ｂ２Ｄ２Ａ１５３６１Ｆで識別される通信機器が接続されている場合である。

【００４８】本実施形態に係る中継機器１０ａによれば、複数の接続ポートのそれぞれに対して、複数の接続ポートのそれぞれにおける通信を許可する通信機器を制限することにより、所定の接続ポートにおいては所定の通信機器による通信のみを許可することができるため、不正進入に対するセキュリティが非常に高いコンピュータネットワークシステムを実現することができる。

【００４９】図４は、コンピュータネットワーク１００とコンピュータネットワーク２００との構成の一例を示す。コンピュータネットワーク１００は、図１に示した構成と同様である。コンピュータネットワーク２００は、コンピュータネットワーク２００における通信を中継するスイッチングハブ等の中継機器１０ｃと、コンピュータネットワーク２００において通信を行う通信機器３０ｅ及び３０ｆとを備える。コンピュータネットワーク１００とコンピュータネットワーク２００とは、セグメントが異なり、ブリッジ、ルータ等の中継機器４０を介して接続される。

【００５０】通信機器３０ａを使用するユーザが、中継機器１０ａの保持部１０２ａに不揮発性メモリを挿入する。そして、中継機器１０ａは、通信機器３０ａのコンピュータネットワーク２００における通信を許可させるべく、不揮発性メモリから読み出した通信機器３０ａを識別する機器識別情報を、中継機器１０ｂを介して中継機器４０に送信する。そして、中継機器４０は、中継機器１０ａから受信した機器識別情報で識別される通信機器３０ａの中継機器４０における通信を許可する。そして、通信機器３０ａは、セグメントが異なるコンピュータネットワーク２００が有する通信機器３０ｅ及び３０ｆと通信することができる。

【００５１】本実施形態に係る中継機器１０ａによれば、通信機器のユーザは、当該通信機器に直接接続される中継機器に不揮発性メモリを挿入することにより、当該通信機器が属するセグメントと異なるセグメントのコンピュータネットワークへの進入を可能にすることができる。

【００５２】図５は、管理装置２０のハードウェア構成を示す。管理装置２０は、ＣＰＵ７００と、ＲＯＭ７０２と、ＲＡＭ７０４と、通信インタフェース７０６と、ハードディスクドライブ７０８と、データベースインタフェース７１０と、フロッピーディスクドライブ７１２と、ＣＤ－ＲＯＭドライブ７１４とを備える。ＣＰＵ７００は、ＲＯＭ７０２及びＲＡＭ７０４に格納されたプログラムに基づいて動作し、各部の制御を行う。通信インタフェース７０６は、コンピュータネットワークを介して中継機器１０ａと通信する。データベースインタフェース７１０は、データベースへのデータの書込、及びデータベースの内容の更新を行う。

【００５３】フロッピーディスクドライブ７１２は、フロッピーディスク７２０からデータ又はプログラムを読み取り通信インタフェース７０６に提供する。ＣＤ－ＲＯＭドライブ７１４は、ＣＤ－ＲＯＭ７２２からデータ又はプログラムを読み取り通信インタフェース７０６に提供する。通信インタフェース７０６は、フロッピーディスクドライブ７１２又はＣＤ－ＲＯＭドライブ７１４から提供されたデータ又はプログラムを中継機器１０ａ送信する。データベースインタフェース７１０は、各種データベース７２４と接続してデータを送受信する。

【００５４】中継機器１０ａに提供されるプログラムは、フロッピーディスク７２０又はＣＤ－ＲＯＭ７２２等の記録媒体に格納されて利用者によって提供される。記録媒体に格納されたプログラムは圧縮されていても非圧縮であってもよい。プログラムは記録媒体から読み出され、通信インタフェース７０６を介して、中継機器１０ａにインストールされ、中継機器１０ａにおいて実行される。

【００５５】記録媒体に格納されて提供されるプログラム、即ち中継機器１０ａにインストールされるプログラムは、機能構成として、読出モジュールと、設定モジュールと、復号モジュールと、送信モジュールと、記憶モジュールと、通信制御モジュールとを有する。各モジュールが中継機器１０ａに働きかけて行わせる動作は、図

１から図４において説明した中継機器１０ａにおける、対応する部材の動作と同一であるから、説明を省略する。

【００５６】図５に示した、記録媒体の一例としてのフロッピーディスク７２０又はＣＤ－ＲＯＭ７２２には、本出願で説明した全ての実施形態における中継機器１０ａの動作の一部又は全ての機能を格納することができる。

【００５７】これらのプログラムは記録媒体から直接中継機器１０ａによって読み出されて実行されても、中継機器１０ａにインストールされた後に中継機器１０ａにおいて実行されてもよい。更に、上記プログラムは単一の記録媒体に格納されても複数の記録媒体に格納されてもよい。又、符号化した形態で格納されていてもよい。

【００５８】記録媒体としては、フロッピーディスク、ＣＤ－ＲＯＭの他にも、ＤＶＤ、ＰＤ等の光学記録媒体、ＭＤ等の光磁気記録媒体、テープ媒体、磁気記録媒体、ＩＣカードやミニチュアカードなどの半導体メモリ等を用いることができる。また、専用通信ネットワークやインターネットに接続されたサーバシステムに設けたハードディスク又はＲＡＭ等の格納装置を記録媒体として使用し、通信網を介してプログラムを中継機器１０ａに提供してもよい。このような記録媒体は、中継機器１０ａを製造するためのみに使用されるものであり、そのような記録媒体の業としての製造及び販売等が本出願に基づく特許権の侵害を構成することは明らかである。

【００５９】以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施形態に記載の範囲には限定されない。上記実施形態に、多様な変更又は改良を加えることができる。そのような変更又は改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【００６０】

【発明の効果】上記説明から明らかなように、本発明によれば、不正進入に対するセキュリティが非常に高いコンピュータネットワークシステムを実現できる中継機器を提供することができる。

【図面の簡単な説明】

【図１】コンピュータネットワーク１００の構成図である。

【図２】中継機器１０ａの構成図である。

【図３】記憶部１１０に格納される通信制御ファイルのデータフォーマットである。

【図４】コンピュータネットワーク１００とコンピュータネットワーク２００との構成図である。

【図５】管理装置２０のハードウェア構成図である。

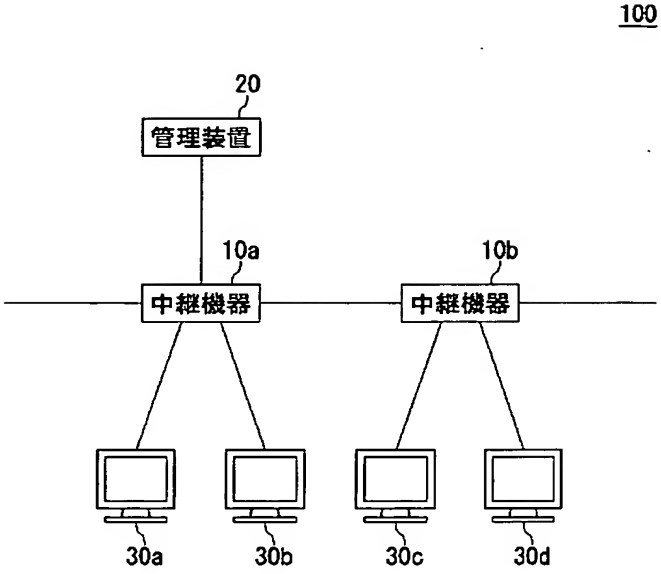
【符号の説明】

１０ａ～１０ｃ　中継機器
２０　管理装置
３０ａ～３０ｆ　通信機器
４０　中継機器
１００　コンピュータネットワーク
１０２ａ～１０２ｆ　保持部
１０４　読出部
１０６　復号部
１０８　設定部
１１０　記憶部
１１２　送受信部
１１４　通信制御部
１１６ａ～１１６ｆ　接続ポート
２００　コンピュータネットワーク
７００　ＣＰＵ
７０２　ＲＯＭ
７０４　ＲＡＭ
７０６　通信インタフェース
７０８　ハードディスクドライブ
７１０　データベースインタフェース
７１２　フロッピーディスクドライブ
７１４　ＣＤ－ＲＯＭドライブ
７２０　フロッピーディスク
７２２　ＣＤ－ＲＯＭ
７２４　各種データベース

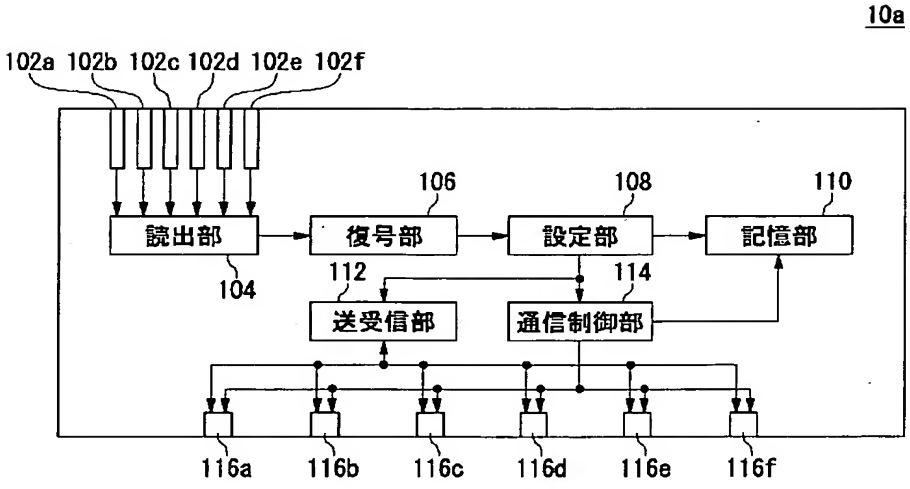
【図３】

接続ポート番号	機器識別情報
1	1A251F33262D
2	3F3610152A1B
3	
4	2B1A392A181C
5	
6	1C2A361F253B, 2B2D2A15361F

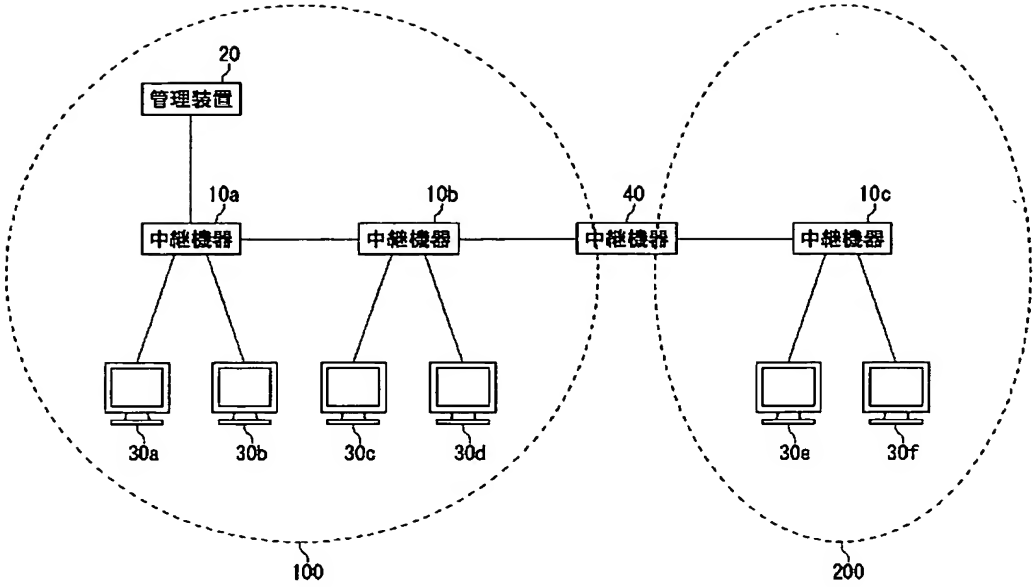
【図１】


100
20
管理装置
10a
10b
中継機器
中継機器
30a
30b
30c
30d

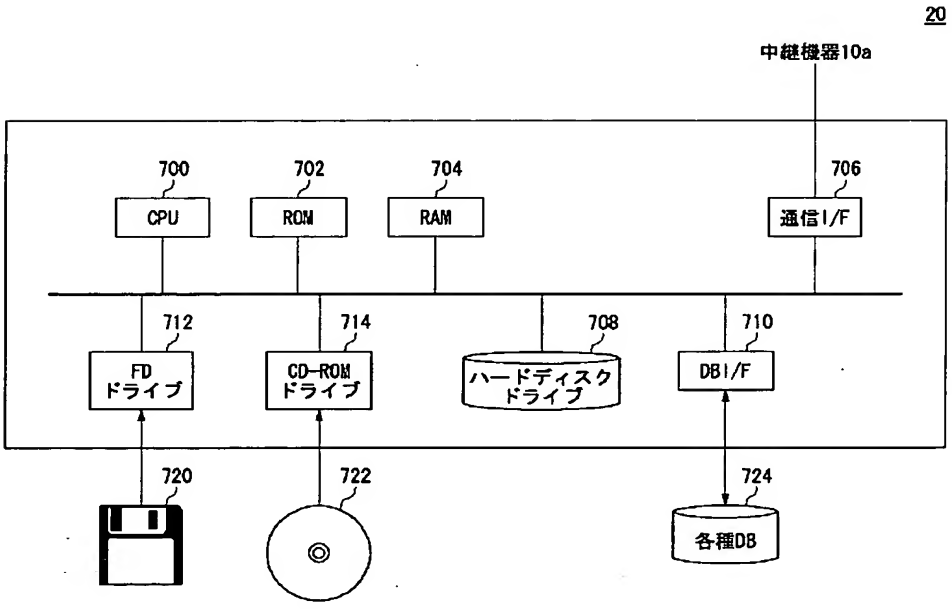
【図２】


10a
102a 102b 102c 102d 102e 102f
106
108
110
読出部
復号部
設定部
記憶部
104
112
114
送受信部
通信制御部
116a
116b
116c
116d
116e
116f

【図４】



【図５】



フロントページの続き